DIRECTOR OF CENTRAL INTELLIGENCE
Security Committee

SECOM-D-254

25 June 1980

MEMORANDUM FOR: Members, DCI Security Committee

STATINTL FROM: [redacted]
Executive Secretary

SUBJECT: Alarm Transmission Line Security

Attached for your information is a copy of a memorandum to the Chairman from the Justice member advising of problems with GSA installed alarm systems. Those departments and agencies with alarm transmission line supervision systems which were installed by GSA may wish to have them inspected to ensure that they provide the expected degree of security.

STATINTL

[redacted]

Attachment

DOJ Review Completed

UNITED STATES DEPARTMENT OF JUSTICE

WASHINGTON, D.C. 20530

Address Reply to the
Division Indicated
and Refer to Initials and Number

June 6, 1980

MEMORANDUM TO: [redacted] Chairman STATINTL
DCI Security Committee

FROM: D. Jerry Rubino
Director of Security
Department of Justice

SUBJECT: Alarm Transmission Line Supervision
(High Security Line Supervision)

The purpose of this memorandum is to alert you, as the Chairman of the DCI's Security Committee, to a potential problem regarding the above-captioned subject.

Recently, the Security Staff of the Department of Justice requested that the General Services Administration (GSA) install alarm systems in the Attorney General's Office and the Associate Attorney General's Office. Specific attention was directed towards ensuring that both alarm systems were protected with an alarm transmission line supervision (or high security line supervision) system pursuant to current U.S. Intelligence Community physical security directives. GSA assured members of my staff that these systems were protected with the most up-to-date systems available, specifically, "a pseudo-random digital tone, double AA high security line supervision system."

During the installation of these systems it became increasingly apparent that the GSA alarm technicians did not truly understand alarm transmission line supervision. As a result, the Department requested GSA to inspect all alarm systems protecting SCI areas and to verify that these areas are, in fact, correctly protected.

OS 0 1518

The results of this inspection ar[illegible] disturbing. Eighty(80) per cent of the GSA install[illegible]m systems in the Department which protect Sensitive [illegible]tmented Information facilities are not equippe[illegible] the requisite alarm transmission line supervisi[illegible]em, even though we requested such service in w[illegible]nd are paying for same. Further, GSA did not[illegible]t to offer any explanation or excuse for their fa[illegible]o properly install the systems as designed by the[illegible]ty Staff.

Based on this recent experience,[illegible]eve it is imperative that all GSA installed alarm s[illegible]s which protect areas that house National Secu[illegible]nformation (NSI) and Sensitive Compartmented Info[illegible]n (SCI) be the subject of close scrutiny by SECOM[illegible]ies to determine the adequacy of such systems.

Due to the severity of this proble[illegible] possible impact on the protection of NSI/SCI in[illegible]ion, you may wish to alert all SECOM members.

CONFIDENTIAL

SECOM-D-252

24 June 1980

MEMORANDUM FOR: Chairman, APEX Steering Group

25X1 FROM: [redacted]
Panel 4

SUBJECT: Report of Activities [redacted] 25X1

1. This memorandum is offered in satisfaction of the tasking of Panel 4. The Panel members representing Navy, Air Force and DIA met on 12 June 1980 and, following examination of the issues of concern arrived at a mutually agreeable and viable course of
25X1 action within the context of the APEX Special Access Control System. [redacted]

2. The essential points of concern are associated with historical needs to limit access to sensitive aspects of national programs balanced by a desire to gain recognized security benefits derived from limited application of compartmentation practices. Over time, project managers have arrived at a workable position. APEX procedures present a perception of possible disruption of this position by requiring revelation of relationships, associations and purposes in greater detail than heretofore. [redacted] 25X1

3. Specifically it was recognized that there is a graded continuum of need-to-know in the large programs. There are decreasing requirements for knowledge about and access to substance and content of national programs as one moves further from the seat of government to peripheral contributors in the industrial environment. The needs for access are least in the "tin bending" population, identified as those individuals currently included under the extended interest of some compartmentation programs. Their activities are first echelon contributions in the manufacturing process. But their activities in isolation are compatible with activities of a similar endeavor intended for nonintelligence application. In and of themselves these activities are not revealing of the nature, purpose or scope

25X1

CONFIDENTIAL

[redacted]

of the program, are not revealing in most cases of final application and may not be classifiable out of context.

25X1 [redacted]

4. It was agreed that such populations could and should be identified by the program manager and a value judgment should be made by him whether or not the activity and hence the associated population meets the criteria for inclusion in the APEX System. 25X1 [redacted]

5. If the Program manager finds for inclusion, then the degree of access that would be required needs to be determined, and only that information necessary to securely accomplish the task would be provided. Procedural briefings would be minimal, and revelation of substantive data would be limited to the essentials without which the tasking could not be accomplished. 25X1 [redacted]

6. If the Program manager finds for exclusion from the APEX System then other noncompartmented security procedures may be adopted and applied at his discretion. [redacted] 25X1

7. In recognition that flexibility is a concomitant of sound security practices, it was acknowledged and agreed that Program managers should retain the authority to elect to seek APEX System protection in the course of a program effort although original evaluation did not so advise. While not specifically addressed during Panel 4 discussions, this concept could apply to discrete operational developmental activities which are clearly "in-house" programs that require no widespread Community knowledge. Formalization into APEX operational compartments would be sought when a need develops for user interface. [redacted] 25X1

8. In connection with the existing draft of the proposed uniform nondisclosure agreement, some concern was expressed that its mention of the Director of Central Intelligence could be erroneously interpreted with undesirable results in those industrial elements considered to be just within the boundary of the APEX System. No solution was proposed for this concern. However, it was acknowledged and agreed that personnel selected as requiring access to material protected by the APEX System would be required to execute APEX nondisclosure agreement. [redacted] 25X1

9. The following recommendations are offered the Chairman and Members of the APEX Steering Group by Panel 4.

1. Program Managers be tasked to review extant compartmentation programs and determine what requires APEX Operational Compartment protection and what does not. Tests for classification as provided in E.O. 12065 and criteria for compartmentation under APEX must be met.

2. Program Managers be tasked to apply need-to-know in briefing personnel performing those activities determined to be within the purview of APEX compartmentation. Only that information pertaining to the compartmented operational project which is essential to secure accomplishment of the task will be revealed. APEX nondisclosure agreements will be obtained.

3. Program Managers be allowed flexibility in timing of petitioning for APEX protection, recognizing that original evaluation may not have sought such protection and that subsequent progress may warrant a different finding for developing projects. [redacted] 25X1

10. The members of Panel 4, listed below, unanimously concur in this report and offer it in satisfaction of the tasking. It is proposed that its recommendations be endorsed by the members and approved by the Chairman, APEX Steering Group for adoption of its precepts by Program Managers as a corollary to the APEX Special Access Control System. [redacted] 25X1

[redacted] 25X1

Chairman

Panel 4 Members:
Robert M. McElroy, Navy
Rollie Kubiskey, Navy
Robert S. Andrews, AF
25X1 [redacted], DIA
Maynard Anderson, OSD
25X1 [redacted] APEX Control Staff

Distribution:
Orig - Addressee
1 ea.- Panel 4 Members
1 - Adm. Showers, O/SA/DCI/CI
1 - SECOM Chrono
1 - SECOM Subject

25X1 SECOM/[redacted]:fh (6/24/80)